REMARKS

In the first office action that was mailed on 04/02/2004 claims 1, 2, 4-13 and 20-46 were rejected under 35 U.S.C. 102(b) as being anticipated by Chi (U.S. 5,978,917), claim 3 was rejected under 35 U.S.C. 103(a) as being unpatentable over Chi, and further in view of Chambers (U.S. 5,398,196), and claims 14-19 were rejected under 35 U.S.C. 103(a) as being unpatentable over Chi. A response was filed on 04/16/2004, wherein none of the claims were amended.

The Examiner has now rejected claims 1, 2 and 4-46 under 35 U.S.C. 103(a) as being unpatentable over Chi and further in view of the newly cited McLain, Jr. (U.S. 5,812,826, hereinafter referred to simply as "McLain"). Claim 3 is now rejected under 35 U.S.C. 103(a) as being unpatentable over Chi and McLain, and further in view Chambers (U.S. 5,398,196). These rejections are respectfully disagreed with, and are traversed below. No claim amendments are made herein, and the following arguments are made with respect to the claims as filed..

It is again noted that Chi and Chambers are referenced on page 2 of the Specification, where it is stated:

> "...U.S. Patent Nos. 5,398,196 and 5,978,917 teach the use of emulation in the analysis of potentially-malicious software. However, these prior art systems do not specifically involve an analysis of network-dependant behavior, or the emulation of activity or services on a network."

The same argument is now again repeated, again incorporated by reference, and further developed below in support of the contention of the Applicants that claims 1-46, as filed, are patentable over Chi in view of McLain, with or without a consideration of Chambers.

With regard to claim 1, the Examiner refers to col. 4, lines 45-66, of Chi for purportedly teaching:

> "a network emulation component, coupled to [said isolated] the network, for

> emulating the behavior of at least a host providing network services; wherein said execution component and said network emulation component cooperate with [said isolated] the network in order to elicit a behavior of the software program that is detectable by said monitoring component." (modifications made by the Examiner to the claim language of claim 1).

It is again pointed out that what is actually stated at col. 4, lines 45-66 is the following:

> "FIG. 4 illustrates apparatus by which the present invention detects and eliminates macro viruses. Emulator 15 is located within computer 1 and executes from within computer 1. Emulator 15 is coupled to the documents 11 generated by application program 5 and to global environment 13. Coupled to emulator 15 is detection module 17, which determines whether a macro virus is present based upon a preselected criterion or preselected criteria. Detection module 17 is coupled to user interface 7, so that it may announce its decisions concerning detection of macro viruses to the user. Coupled to detection module 17 is repair module 19, which eliminates macro viruses that have been determined by detection module 17 to be present. Since these viruses can appear in any document 11 or in the global environment 13, repair module 19 is coupled to all of the documents 11 and to global environment 13.
>
> In general, emulator 15 works by first emulating all of the tested macros assuming that they are located in global environment 13. All copies of macros to a local document 11 are noted. Then emulator 15 emulates the execution of all of the tested macros assuming that they are located in a local document 11."

The "global environment" is defined in col. 2, at lines 26-31, as being:

> "an area within a storage medium that is associated with a particular application program and stores parameters and/or macros with said application program. For example, the global environment for a particular application program can contain text, graphics, and one or more macros."

In view of the foregoing, it is respectfully submitted that there is no mention in Chi of a "network emulation component", coupled to a network (isolated or otherwise) for "emulating the behavior of at least a host providing network services" where the execution component and "said network emulation component" cooperate with the network (isolated or otherwise) in order to "elicit a

behavior of the software program that is detectable by said monitoring component."

The Examiner now uses McLain for purportedly teaching "said execution component being coupled to an isolated network that does not have a direct connection to another network that is not an isolated network" as in claim 1, and has then stated that it would have been obvious to combine Chi's system for the detection and elimination of macro viruses with McLain's method for emulating network monitoring devices "in order to allow realistic monitoring and control systems testing prior to actual implementation (McLain col. 2 lines 53-65)".

This rejection is respectfully disagreed with.

The full text of col. 2, lines 53-65 of McLain is as follows:

> "What is needed is a computer-implemented method and apparatus for emulating an entire COS report network to allow realistic MCS testing prior to actual implementation. The complete range of functionality of an MCS needs to be stressed. Communication between the MCS and a report network covering millions of alarm points needs to be emulated for different report network configurations, events, and COS indications."

The COS is a Change-of-State alarm module that forms part of a commercially available state monitoring device (DL 10) employed in a network of state monitoring devices, where the DL 10 is a Datalok device manufactured by Pluscom, and where the MCS is a monitoring and control system (see col. 1, lines 50-65).

What is also stated at col. 2, lines 36-57, of McLain is the following:

> "To test the software, hardware, and communications of such an MCS, the behavior of DL 10 devices must be mimicked. To use an actual network of DL 10 devices in a test environment to test the MCS would be impractical; a typical network may consist of hundreds and even thousands of DL 10 devices. To emulate a small sample of the network would not provide the stress and volume needed to fully test the complete range of functionality of the MCS.
>
> To fully test MCS performance, the MCS must be stressed by the behavior of an

> entire COS report network. As discussed above, a typical report network, such as, a Datalok 10 report network manufactured by Pluscom, can include 16 links to over 4000 state monitoring devices covering over two million alarm points. Given this complexity, to use an actual report network of state monitoring devices in a test environment to fully-test an MCS is impractical and cost-prohibitive.
>
> Prior to the present invention, the behavior of a COS report network has not been fully emulated to test a MCS. Network behavior has not been emulated on any scale to test an MCS, especially in an environment where processing power is limited as in a personal computer system."

The purpose of any emulation that affects a network in McLain is thus clearly in the context of emulating the behavior of a Change-of-State (COS) report network in a Monitoring and Control System (MCS).

Further, the concept of an "isolated network" is not found in McLain. In fact, the only mention of "isolation" is found in the Summary at col. 3, lines 28-37, where it is stated that:

> "Invalid messages representing corrupt data sent by individual state monitoring devices and other communication misbehavior can also be emulated in a controlled and repeatable environment. All inbound and outbound communication messages are logged to a communication log file for further analysis. Self-monitoring status and/or error messages are logged to a self-diagnostic file to improve trouble-shooting, error tracing, and isolation of any anomalies during emulation" (emphasis added).

That portion of McLain referred to by the Examiner for purportedly teaching "said execution component being coupled to an isolated network that does not have a direct connection to another network that is not an isolated network" as in claim 1 is col. 3, lines 11-18. However, all that is disclosed by McLain is the following:

> "An advance in the ability to test an MCS is obtained by emulating the behavior of a report network in reporting detected changes-of-state for a full complement of state monitoring devices. Communication between the MCS and a report network emulator of the present invention is emulated to match actual communication between the MCS and the emulated report network."

What this portion of McLain has to do with an "execution component being coupled to an

isolated network that does not have a direct connection to another network that is not an isolated network" is not at all understood.

Still further, and as is specifically stated by McLain at col. 6, lines 16-19, the:

> "network can be any configuration or interconnection of state monitoring devices. The COS report network being emulated can support over four thousand network state monitoring devices."

As was argued above, it is not seen where there is any mention in Chi of a "network emulation component", coupled to a network (isolated or otherwise) for "emulating the behavior of at least a host providing network services", where the execution component and "said network emulation component" cooperate with the network (isolated or otherwise) in order to "elicit a behavior of the software program that is detectable by said monitoring component", and there is also clearly no express or implied disclosure in McLain of an "execution component being coupled to an isolated network" (of state monitoring devices?) "that does not have a direct connection to another network" (of state monitoring devices?) "that is not an isolated network" (of state monitoring devices?), as in claim 1.

It is respectfully submitted that there would not be any incentive for one skilled in the art to attempt to combine the teachings of Chi and McLain and, furthermore, even if such a combination were attempted (which is not admitted is suggested), it is not seen how any result of such a combination (which would presumably have the document-based macro virus detection and elimination system of Chi somehow grafted onto the system of McLain that uses emulation of the behavior of the Change-of-State (COS) report network (of state monitoring devices) in the Monitoring and Control System (MCS)) would render the claims unpatentable under 35 U.S.C. 103(a).

Further, it is not understood why one skilled in the art would wish to combine Chi's system for the **detection and elimination of macro viruses in documents 11** with McLain's method for emulating a network of state monitoring devices "**in order to allow realistic monitoring and**

control systems testing prior to actual implementation (McLain col. 2 lines 53-65)", as stated by the Examiner. Clarification is requested.

In that claim 1 is clearly patentable over Chi in view of McLain, then claims 2-26 are also patentable.

Further in this regard, and by example only, the Examiner points to Chi at col. 3, lines 36-40 and 49-52, with regard to claim 24, that further modifies claim 23. Claim 23 recites in part that the "monitoring component comprises at least one event handler programmed so as to obtain control when certain events or types of events occur", and claim 24 recites that "the certain events or types of events comprise at least one of creation of a new file in a filesystem, a receipt of mail, an opening of mail, a posting of news, an opening of a new socket connection, an execution of a particular application, and an alteration of a system registry". However, in col. 3, lines 36-40 and 49-52, Chi discusses only the basic operations of Microsoft Word and Excel with regard to generating and opening documents. It is not at all clear what this has to do with the subject matter claimed in claim 24, in particular in the manner in which it further modifies the subject matter of claim 23.

The foregoing arguments apply as well to independent claim 27, which is drawn to a system for eliciting a desired behavior from a software program, where the system comprises:

> "an emulated data communications network having at least one emulated network server coupled thereto, said at least one emulated network server responding to requests received from said emulated data communications network;
>
> an emulated host computer coupled to said emulated data communications network, said emulated host computer for executing the software program, the software program operating to originate requests to said emulated data communications network;
>
> at least one emulated goat computer coupled to said emulated data communications network; and
>
> at least one monitor for detecting an occurrence of the desired behavior in at least

> one of said emulated network server, said emulated host computer, and said at least one emulated goat computer." (emphasis added)

It is respectfully submitted that at least the highlighted subject matter shown above is not found in, is not disclosed in, and is not suggested by Chi in view of McLain, and the Examiner has not specified where this subject matter would be found. As but one example, it is not understood where either Chi or McLain disclose or suggest the presence of "at least one emulated goat computer coupled to said emulated data communications network; and at least one monitor for detecting an occurrence of the desired behavior in at least one of said emulated network server, said emulated host computer, and said at least one emulated goat computer."

In that claim 27 is clearly not rendered obvious by the proposed combination of Chi in view of McLain, then for at least this one reason alone the dependent claims 28-36 are also clearly patentable over Chi in view of McLain.

Independent claim 37 is drawn to a computer program embodied on at least one computer-readable medium for executing a method for eliciting a behavior from a software program. In claim 37 the method is said to comprise:

> "emulating a data communications network having at least one emulated network server coupled thereto, said at least one emulated network server operating to respond to requests received from said emulated data communications network;
>
> emulating a host computer coupled to said emulated data communications network, said emulated host computer executing the software program, the software program operating to originate requests to said emulated data communications network; and
>
> detecting an occurrence of the behavior in at least one of said emulated network server and said emulated host computer."

It is also respectfully submitted that at least the highlighted subject matter shown above is not found in, is not disclosed in, and is not suggested by the system described by Chi in view of

McLain. If the Examiner believes otherwise then he is respectfully requested to specifically point out where these elements are disclosed in Chi and/or McLain.

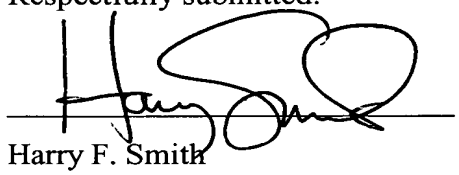
Further, since these various claimed elements are not found in Chi in view of McLain, then for at least this one reason alone the dependent claims 38-46 are also clearly patentable over Chi in view of McLain.

The addition of Chambers does not render claim 3 unpatentable, at least for the reason that claim 3 depends from a clearly allowable claim 1.

The foregoing arguments have concentrated primarily on the patentability of the independent claims 1, 27 and 37 and, in so doing, have simultaneously and clearly established the patentability of the dependent claims. However, should the Examiner persist in maintaining this rejection, the Applicants reserve the right to argue the patentability of each of the dependent claims individually.

The Examiner is respectfully requested to reconsider and remove the expressed rejections, and to allow claims 1-46 as originally filed. However, should there be any remaining issue that would impede the allowance of all of the pending claims, then the Examiner is respectfully requested to contact the undersigned attorney through any of the means set forth below.

Respectfully submitted:



11/2/2004

Harry F. Smith — Date

Reg. No.: 32,493
Customer No.: 29683
HARRINGTON & SMITH, LLP
4 Research Drive
Shelton, CT 06484-6212
Telephone: (203)925-9400 Facsimile: (203)944-0245

S.N. 09/640,453
Art Unit: 2137

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

11/2/04 — Ann Obrentowich

Date — Name of Person Making Deposit